Heikki Tuononen

IT-infrastruktuurin valvontajärjestelmät

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietoverkot

Insinöörityö

15.1.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Heikki Tuononen IT-infrastruktuurin valvontajärjestelmät 39 sivua 15.1.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Tuotantopäällikkö Aleksi Airaksinen Yliopettaja Janne Salonen

Insinöörityössä oli tavoitteena kartoittaa Appelsiini Finland Oy:n tarpeet IT-infrastruktuurin valvontajärjestelmälle. Lisäksi haluttiin tutkia, miten käyttäjät kokevat nyt käytössä olevan järjestelmän ja onko sille tarjolla teknisesti varteenotettavia vaihtoehtoja kaupallisissa tuotteissa.

Tarvekartoitus tehtiin haastattelemalla valvonnasta vastaavaa asiantuntijaa sekä muutamia muita Appelsiinin työntekijöitä ylläpidosta ja palvelunhallinnasta. Nykyistä järjestelmän käytettävyyttä arvioitiin muutaman ylläpitäjän haastattelujen pohjalta sekä omiin kokemuksiin pohjautuen. Markkinakartoitus tehtiin hakemalla internetistä tietoa valvontajärjestelmistä ja niiden toimittajista ja valitsemalla asetetut kriteerit parhaiten täyttävät järjestelmät lähempään tarkasteluun. Tekniset ominaisuudet kerättiin pääosin tuotteiden manuaaleista ja markkinointimateriaaleista.

Kartoitus osoitti, että markkinoilla on runsaasti erilaisia ilmaisia ja maksullisia valvontajärjestelmiä, joista palvelutuotantoon sopivia on vain murto-osa. Tuotteiden vertailussa selvisi, että teknisiltä ominaisuuksiltaan nykyinen valvontajärjestelmä Nimsoft Monitor on varsin kilpailukykyinen ja parannusta olisi mahdollista saada lähinnä käyttöliittymään.

Avainsanat	Verkonvalvonta, järjestelmänhallinta

Author(s) Title Number of Pages Date	Heikki Tuononen Monitoring systems for IT infrastructure 39 pages 15.1.2014
Degree	Bachelor of Engineering
Degree Programme	Degree Programme in Information Technology, Communication and Data Networks
Specialisation option	Data Networks
Instructor(s)	Aleksi Airaksinen, Production Manager Janne Salonen, Principal Lecturer

The objective of the study was to define what sort of needs for network monitoring system does Appelsiini Finland Oy have. An equally important objective was to evaluate the current monitoring system and whether there are alternative technically comparable systems available.

To find out the needs for the monitoring system Appelsiini employees from systems administration and service management were interviewed. The usability of the current monitoring system was evaluated based on interviews and personal experience working with the system. The market research was conducted by searching information about available systems and vendors online and then selecting the systems meeting Appelsiini's criteria to be reviewed and compared in detail. The technical data was gathered using product manuals and various marketing materials.

The survey revealed that even though there is an abundant supply of monitoring systems there are only few products that are actually suitable for service production. The technical comparison of the products suggested that the current monitoring system, Nimsoft Monitor, is able to match or outperform its competitors in most aspects. By changing the system supplier the benefits would be primarily seen in the user interface.

Keywords	Network monitoring, system management

Sisällys

Lyhenteet

API	Application programming interface eli ohjelmointirajapinta. Määrittelee, kuinka ohjelmistokomponentit voivat viestiä keskenään.
CI	Configuration item eli konfiguraation rakenneosa. IT-palvelun toimittamiseen käytettävä komponentti tai muu resurssi, joka tallennetaan konfiguraationhallintatietokantaan (CMDB).
CMDB	Configuration management database. Konfiguraatiotietokanta. Tietokanta, joka sisältää tiedot konfiguraation rakenneosista läpi niiden elinkaaren.
GUI	Graphical user interface eli graafinen käyttöliittymä.
HA	High availability eli korkea saatavuus. Suunnitteluratkaisuilla pyritään tarjoamaan mahdollisimman katkoton palvelu.
OSI-malli	Open systems interconnect model on ISO:n viitemalli, joka jakaa tiedonsiirtoprotokollat seitsemään kerrokseen.
QoS	Quality of service eli palvelunlaatu.
SaaS	Software as a service eli sovelluksen hankinta palveluna perinteisen lisenssin hankinnan sijasta.
SNMP	Simple network management protocol eli yksinkertainen verkonvalvontaprotokolla. Käytetään verkkolaitteiden valvontaan ja rajoitetusti myös konfigurointiin.

1 Johdanto

Työn tarkoituksena on kartoittaa työn tilaajan, Appelsiini Finland Oy:n, tarpeet ja vaatimukset it-infrastruktuurin valvontajärjestelmälle. Lisäksi selvitetään, miten markkinoilla olevat järjestelmät vastaavat työssä määritettyjä vaatimuksia. Tilaaja käyttää kartoitusta valitessaan yrityksen käyttöön tulevan valvontajärjestelmän.

Appelsiini Finland Oy on monipuolisesti IT-palveluita tuottava yritys, joka työllistää tällä hetkellä noin 300 henkilöä ja palvelee keskisuuria ja suuria yrityksiä pääosin Suomessa. Niin yrityksen asiakkailleen tuottamat perustietotekniikan palvelut, esimerkkeinä palvelinten ja tietoliikenneverkkojen ylläpito, kuin yrityksen sisäisten järjestelmien ja laitteiden ylläpitokin vaativat automatisoidun valvontajärjestelmän käyttöä. Valvontajärjestelmä tarkkailee jatkuvasti laitteiden ja sovellusten tilaa ja tarvittaessa antaa hälytyksen, kun se havaitsee poikkeaman tai virheen. Koska IT-ympäristön katkottoman toiminnan takaaminen on juuri se, mitä asiakkaille myydään, on valvontajärjestelmä useissa tapauksissa kriittisessä asemassa liiketoiminnan tavoitteiden saavuttamiseksi. Valvontajärjestelmä on tarpeen myös palveluiden laadun seurannassa ja asiakasraportoinnissa.

Tutkimuksen alussa selvitetään lyhyesti valvontajärjestelmien tarkoitus, käyttökohteet ja toiminta. Seuraavaksi luodaan katsaus Appelsiinin nykyiseen valvontajärjestelmään ja erityisesti siinä havaittuihin puutteisiin tai ongelmiin. Tutkimuksen ydin on yrityksen eri tahojen järjestelmälle asettamien vaatimusten ja toiveiden selvittäminen ja kootun määrittelyn vertaaminen markkinoilta löytyviin tuotteisiin. Kaikkia ominaisuuksia ei voi kuitenkaan arvioida pelkästään saatavissa olevien dokumenttien ja esittelyiden pohjalta ja ilman syvällistä käyttökokemusta, joten monissa kohdin joudutaan turvautumaan faktojen sijasta parhaaseen arvaukseen. Monista järjestelmistä on onneksi saatavilla koekäyttöön ilmainen demoversio, jolla tuotteen sopivuutta voi tutkia tarkemmin. Tutkimuksen lopuksi esitetään yhteenvetona koottuja vaatimuksia parhaiten vastaavat järjestelmät. Kustannuskysymykset on kuitenkin jätetty tämän kartoituksen ulkopuolelle aihealueen koon rajaamiseksi.

2 IT-infrastruktuurin valvonta ja valvontajärjestelmät

Palveluiden yhteydessä IT-alan käytäntökokoelma Information Technology Infrastructure Library eli ITIL kertoo infrastruktuurin koostuvan kaikista niistä laitteista, joilla IT-palveluita tuotetaan [1]. Sovellukset on siis ITIL:ssä rajattu infrastruktuurin käsitteen ulkopuolelle. Tämän selvityksen yhteydessä infrastruktuuriin luetaan kuitenkin kuuluviksi myös sovellukset, koska ne muodostavat yhtä oleellisen osan tuotettavista palveluista kuin fyysiset laitteetkin. Kartoituksen tilaaja myy asiakkailleen pääosin palvelua, joten palvelukeskeinen näkemys on siksikin perusteltu.

Valvonnan yhteydessä on syytä käsitellä myös hallinnan käsite, koska yhdellä järjestelmällä voidaan usein toteuttaa, ainakin osittain, molemmat toiminnot. Tämän selvityksen kannalta oleellisempi toiminto on otsikonkin mukaisesti valvonta, mutta myös hallintaominaisuuksia sivutaan. Tällä hetkellä Appelsiinin käytössä oleva järjestelmä keskittyy lähes yksinomaan valvontaan.

2.1 Valvontajärjestelmien toiminta

Lyhyen historiansa aikana tietotekniset järjestelmät ovat laajentuneet käsittämään valtavia laiteverkostoja, jotka levittäytyvät jopa mantereelta toiselle. Laitteiden ja sovellusten tuottamat palvelut ovat puolestaan muodostuneet käyttäjilleen erittäin tärkeiksi. Esimerkiksi sähköposti on useille yrityksille toimialasta riippumatta tärkeä palvelu ja sen hetkelliseenkin toimimattomuuteen reagoidaan välittömästi. Suuren infrastruktuurin valvonta ei onnistu pelkästään ihmisvoimin, joten itse tuotantojärjestelmän rinnalle tai sen lomaan tarvitaan toinen järjestelmä, joka valvoo keskitetysti ensisijaisen järjestelmän toimintaa. Optimitilanteessa valvontajärjestelmä osaa ilmoittaa poikkeamista jo siinä vaiheessa, kun valvottavan kohteen loppukäyttäjät eivät sitä vielä havaitse ja ongelma ehditään korjata ennen varsinaista virhetilannetta, jolloin voidaan taata palveluiden jatkuvuus. Jotta valvonta kykenee optimisuoritukseensa, on siihen panostettava samalla lailla resursseja kuin muihinkin liiketoiminnalle kriittisiin järjestelmiin.

Valvontajärjestelmän pääkomponentteja ovat tyypillisesti keskuspalvelin, joka valvoo laitteita ja koostaa niistä kertyvää dataa tietokantaan tai muuhun tietorakenteeseen. Tietojen esittämisestä huolehtii käyttöliittymä, joka on yleensä selaimessa toimiva. Datan keruu voi tapahtua agentin avulla tai ilman. Agentti on paikalliseen järjestelmään

asennettava ohjelmisto, joka kerää tietoa halutuista parametreista ja joko lähettää sen eteenpäin tai säilöö noudettavaksi. Agentiton valvonta toimii hyödyntämällä jo olemassa olevia tai aiemmin asennettuja komponentteja kuten käyttöjärjestelmää ja sen rajapintoja, esimerkiksi WMI Windowsissa. Agentiton valvontakin tarvitsee siis jonkinlaisen ohjelmistokomponentin, joka kerää dataa, mutta erona agentilliseen valvontaan on se, että valvonnan kohteeseen ei tarvitse asentaa mitään lisäosia. Agentittoman valvontajärjestelmän etuna on yksinkertaisempi järjestelmäarkkitehtuuri, mikä helpottaa käyttöönottoa ja ylläpitoa. Paikallisella agentilla päästään yleensä valvomaan järjestelmän ominaisuuksia kattavammin ja sillä voidaan myös säilöä mittausdataa paikallisesti esimerkiksi verkkokatkon aikana, jolloin dataa ei huku. Haittapuolena on kasvava ylläpidon tarve esimerkiksi agenttien käyttöönoton ja päivittämisen muodossa.

Tyypillisiä valvottavia infrastruktuurin osia ovat palvelimet, verkkolaitteet kuten kytkimet ja reitittimet sekä eri laitteissa toimivat sovellukset ja palvelut. Valvottavista kohteista kerätään vaihtelevasti dataa, joka koostetaan tarkoituksenmukaiseen muotoon esimerkiksi hetkellisiksi hälytyksiksi tai pidemmän aikavälin raporteiksi. Kerättyä dataa analysoimalla voidaan myös koettaa ennustaa tulevia tapahtumia.

Kerättävä data jakautuu saatavuus- ja suorituskykytietoon. Saatavuutta mitataan esimerkiksi tutkimalla, onko tietty laite päällä tai vastaako jokin palvelu pyyntöihin. Tyypillisiä suorituskyvyn mittareita ovat esimerkiksi prosessorin käyttöaste ja vapaan muistin määrä palvelimissa, verkkoporttien tila ja verkkoliikenteen määrä kytkimissä sekä palvelupyyntöjen vasteaika sovelluspalvelimilla.

Verkonvalvontaan on olemassa oma SNMP-protokollansa (simple network management protocol). SNMP-valvontaa ohjaa valvontajärjestelmä, joka komentaa aktiivilaitteissa toimivia agentteja. Valvottavalla verkkolaitteella on tietovarasto MIB (mangement information base), josta agentti noutaa tietoa tai johon se vie tietoa pyydettäessä. Agentti voi lähettää pyytämättä myös hälytyksen eli trapin. Toinen yleisesti käytetty protokolla on ICMP (internet control message protocol), jonka avulla TCP/IP-verkon laitteille lähetetään ping-kyselyitä, joilla selvitetään, toimiiko verkkoyhteys laitteiden välillä. Verkonvalvontaan kuuluviksi voidaan joskus laskea myös OSI-mallin sovelluskerroksen protokollat, esimerkiksi DNS (domain name system) ja HTTP (hypertext transfer protocol), jotka käyttävät varsinaiseen datan siirtoon UDP- ja TCP-protokollia. Sovelluskerroksen protokollilla on kuitenkin usein käytännöllistä valvoa juuri kyseisten

palveluiden toimintaa, esimerkkinä DNS-palvelimen toiminnan varmistaminen DNS-kyselyillä ja verkkopalvelun toiminnan varmistaminen HTTP-kyselyllä.

Fyysisten laitteiden eli ”raudan” toimintaa valvotaan sen omien antureiden avulla. Esimerkiksi palvelimen emolevy valvoo tyypillisesti jännitteitä, lämpötiloja ja tuulettimien kierrosnopeuksia. Tämä mittausdata ei ole saatavilla ilman lisäohjelmistoa eikä etäluettavissa yleisten rajapintojen kautta. Dataan pääsee käsiksi esimerkiksi laitevalmistajien omilla valvontaohjelmistoilla. Laite- tai valmistajaspesifit ohjelmistot voidaan usein integroida keskitettyyn valvontaan ja saada näin tieto esimerkiksi vikaantuneesta virtalähteestä tai tuulettimesta. Toinen tapa toteuttaa laitevalvontaa on asentaa oma agentti, jolla päästään lukemaan laitteiston antureita.

Sovellusten valvonta on usein mutkikkaampaa ja erittäin sovelluskohtaista. Tyypillisiä valvontakohteita ovat esimerkiksi web-sivun toiminta ja tietokantayhteyden toimivuus. Kolmannen osapuolen toimittaman, tarkemmin räätälöityjen sovellusten valvonnan konfigurointiin tarvitaan usein varsinaisen konfiguroinnin tekijän lisäksi sovelluksen pääkäyttäjän sekä sovelluksen toimittavan palveluntarjoajan apua.

2.2 Valvonnan suunnittelu ja toteutus

Valvottavan infrastruktuurin luonteesta riippuen valvontajärjestelmän suunnittelu ja toteutus on haastavimmillaan kaukana triviaalista. Valvottavat järjestelmät ovat fyysisten laitteiden, ohjelmistojen, verkkojen ja niitä operoivien käyttäjien kudoksia, joiden valvonta ei onnistu pelkästään teknisten määritysten pohjalta. Koska valvonta on keskeinen osa palvelutuotannon toimintaa, sen tuottaman datan on oltava luotettavaa ja toiminnan vikasietoista. Käyttäjien tarpeet vaihtelevat vahvasti roolien mukaan, joten varsinaisen valvontamoottorin lisäksi myös käyttöliittymän on venyttävä erilaisiin tarpeisiin.

Suunniteltaessa valvontajärjestelmää tarvitaan siis laaja-alainen näkemys toimintaympäristöstä ja toisaalta tietoa pienemmistäkin yksityiskohdista. Lisäksi jo suunnitteluvaiheessa on hyvä tietää, mitkä valvottavista järjestelmistä ovat tärkeimpiä. Usein yhdellä henkilöllä ei voi olla tietoa kaikista valvottavista järjestelmistä ja valvontaan liittyvistä sidosryhmistä, joten suunnittelu ja toteutus vaativat yhteistyötä organisaation eri tahojen kesken. Esimerkiksi järjestelmän käyttöympäristöön tulevien muutosten ennakointi

ei välttämättä onnistu parhaiten tekniseltä asiantuntijalta, vaan vaatii tietoa korkeammalla tasolla tehdyistä linjauksista. [2.]

Valvonnalla kerättävä data luo monenlaisia haasteita. Kerätty tieto pitää pystyä säilyttämään riittävän pitkään esimerkiksi raportteja ja ennusteita varten, joten ajan myötä suurissa ympäristöissä kertyy huomattavia määriä dataa. Datan määrä kuormittaa tietokantapalvelimia paitsi tallennustilan myös muiden resurssien osalta. Liiallinen datan keruu kuorimittaa myös verkkoa, kun mittausdata siirretään kohteesta tietokantaan. Tämän vuoksi kaikkea saatavilla olevaa dataa ei ole järkevää kerätä talteen, vaan joudutaan harkitsemaan, mikä tieto on oleellista ja kuinka kauan mitäkin tietoa säilytetään.

Käyttöliittymän kohdalla tiedon määrä on osattava tasapainottaa siten, että mitään tärkeää ei jää huomaamatta, mutta toisaalta informaation määrä ei hukuta hyödyllistä dataa merkityksettömän kohinan sekaan. Käyttöliittymän kustomoitavuus ja datan suodatustoiminnot ovatkin ensisijaisen tärkeitä päivittäisen käyttömukavuuden ja käytön tehokkuuden kannalta.

Raportointi ja sen käyttöliittymä ovat valvontajärjestelmän tärkeä osa erityisesti asiakkaille viestittäessä. Asiakkaan ostamille palveluille on useimmiten määritetty tarkat tavoitetasot, joiden täyttymistä on mitattava ja raportoitava. Palvelutaso (service level) määritetään palvelutasosopimuksessa (service level agreement, SLA), jonka parametrien täyttymistä myös asiakas voi seurata raportointiportaalista. Helppokäyttöinen ja tehokas raporttien koostaminen säästää siis palvelunhallinnan aikaa ja parantaa myös asiakkaiden käyttökokemusta.

Turvallisuus on myös huomioitava kerättäessä ja säilöttäessä massiivisia määriä dataa useiden asiakkaiden ympäristöistä. Data pitää voida siirtää järjestelmien välillä salatussa muodossa, ja sen varastoinnin on oltava turvallista. Asiakkaan salassapitovaatimuksista riippuen myös oman organisaation työntekijöiden pääsyä dataan voidaan joutua rajoittamaan.

Valvontajärjestelmä on vain yksi osa IT-infrastruktuuria, joten sen pitää toimia yhdessä muiden järjestelmien kanssa. Esimerkiksi käyttäjien tunnistaminen voidaan hoitaa Active Directory- tai LDAP-integraation avulla. Valvontajärjestelmän on hyvä integroitua myös työnohjausjärjestelmään. Työnohjausjärjestelmä seuraa ja allokoi työtehtäviä erityyppisillä tiketeillä, jotka kuvaavat esimerkiksi häiriöitä (incident), muutoksia (change) ja ongelmia (problem). Valvontajärjestelmän antamista hälytyksistä generoidaan häiriötikettejä, jotka siirretään lajittelun kautta tukihenkilön tai -ryhmän työjonoon. Mitä enemmän häiriöstä voidaan siirtää tietoa suoraan tikettiin, sitä helpompi tiketti on lajitella oikein ja sitä nopeammin häiriötilanteen selvittäminen voidaan aloittaa. Tiketin käsittelyn kannalta oleellisia hälytyksestä siirrettäviä tietoja ovat esimerkiksi häiriön prioriteetti, rakenneosa (configuration item eli CI) ja tapahtuma-aika.

3 Valvontajärjestelmän nykytilanne

Appelsiinilla on tällä hetkellä kymmeniä asiakkaita ja tuhansia valvottavia laitteita ja järjestelmiä, jotka jakautuvat alikomponentteihinsa. Aiemmin valvontajärjestelmä on ollut avoimen lähdekoodin Nagios, mutta nykyisin käytössä on CA Nimsoft Monitor. Valvontajärjestelmää käyttävät ja hallinnoivat pääasiassa ylläpitäjät, mutta sen toiminta näkyy suoraan lähes kaikille palvelutuotantoon osallistuville tavalla tai toisella.

3.1 CA Nimsoft Monitor

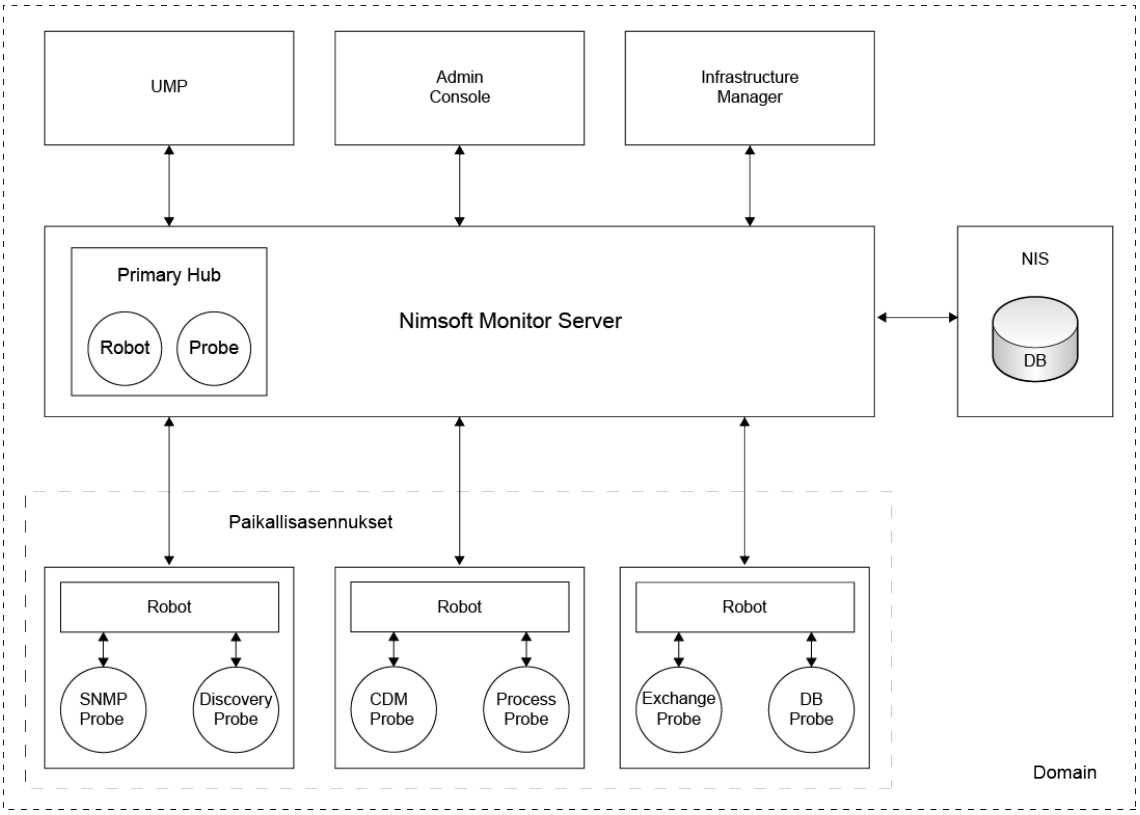
CA Nimsoft Monitor on kaupallinen tuote ja osa CA:n Unified Management -pakettia. Nimsoft on saatavilla palveluna (SaaS) tai asiakkaan omaan ylläpitoon. Valmistajan mukaan Nimsoft on koko IT-infrastruktuurin valvontaan soveltuva, skaalautuva ratkaisu, joka sopii hyvin palveluntarjoajien käyttöön.

Valvottavien järjestelmien listalta ei puutu mitään olennaista. Tärkeimmät Nimsoftilla valvottavat teknologiat kategorioittain ovat:

- käyttöjärjestelmät: Windows, Linux ja Unix
- tallennus: EMC, IBM System Storage ja Netapp
- verkot: kytkimet, reitittimet ja palomuurit SNMP-, ICMP- ja TCP-protokollien avulla

- virtualisointi: VMWare, Hyper-V, XenServer, XenDesktop ja Amazon AWS
- tietokannat: Microsoft SQL Server, MySQL, IBM DB2, Oracle ja Sybase
- sovellukset: Active Directory, Exchange, IIS, Sharepoint, Citrix, JBoss ja SAP
- laitteet: Cisco UCS, IBM Power Systems.

Nimsoftin arkkitehtuuri on esitetty korkealla tasolla kuvassa 1. Kuvassa katkoviivalla rajattu domain eli toimialue on looginen kokonaisuus, joka muodostuu ohjelmiston asennuksen yhteydessä. Domainiin kuuluvat kaikki saman Nimsoft-toteutuksen osat.



Kuva 1. Nimsoft Monitorin komponentit ja niiden ryhmittely domainissa. Kuvassa Monitor Serverin yläpuolella ovat hallintatyökalut ja alapuolella valvottaviin laitteisiin asennettavat osat.

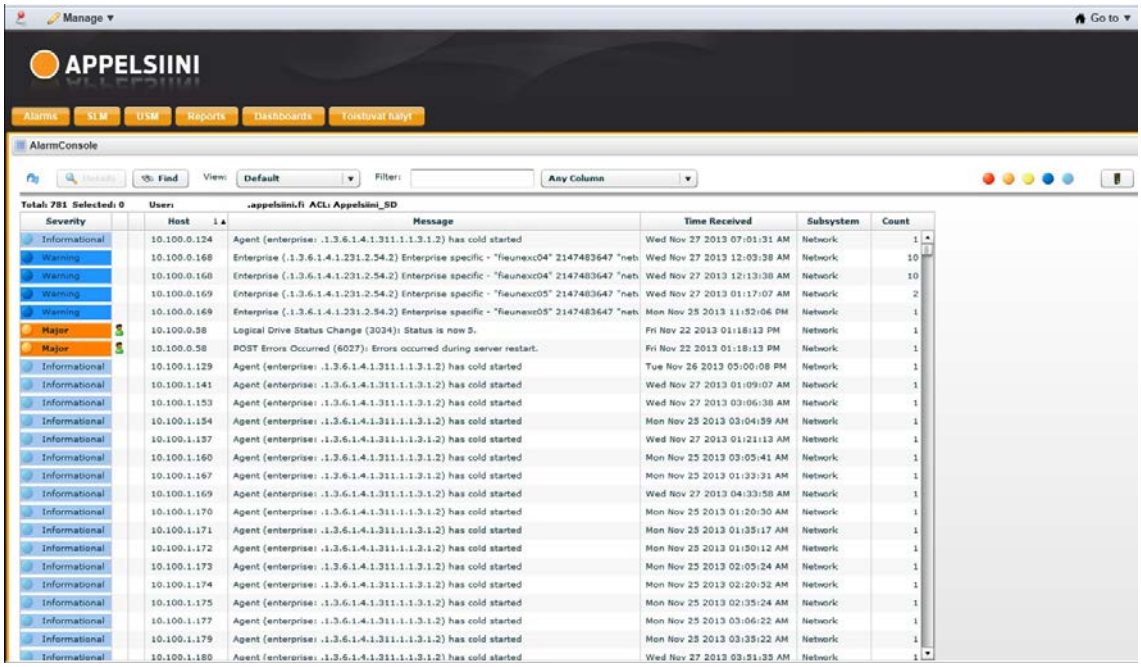
Nimsoft Monitor Server (NMS) on järjestelmän keskuspalvelin ja sisältää keskeisimmät datan keruutoiminnot. Myös tietovarasto eli Nimsoft Information Store (NIS) on NMS:n looginen osa. Järjestelmän käyttöliittymäelementit ovat Infrastructure Manager (IM), Admin Console ja Unified Management Portal (UMP). IM on Windows-pohjainen hallintakonsoli, jonka kautta valvonta-asetukset konfiguroidaan. Admin Console on selaimessa toimiva hallintakonsoli, joka tarjoaa useimmat IM:n toiminnot ilman konsolin

asennusta. UMP on selaimessa toimiva valvontakonsoli, joka tarjoaa näkymiä valvontadataan ja raportteihin sekä rajoitetut hallintamahdollisuudet. [3.]

Nimsoft Monitor Serverin komponentit tarkemmin eriteltyinä ovat:

- Message Bus eli viestiväyläpois tarjoaa viestinvälityspalvelut muille järjestelmän osille.
- Primary Hub eli ensisijainen keskuspalvelin.
- Nimsoft Information Store (NIS) on tietovarastona toimiva tietokanta. Tuettuja alustoja ovat Microsoft SQL Server, MySQL ja Oracle.
- Monitoring infrastructure eli valvontainfrastruktuuri koostuu keskuspalvelimista, roboteista ja probeista.

Nimsoft voidaan asentaa fyysiselle tai virtualisoidulle Windows-, Linux- tai Solaris-alustalle. Suuren 50 hubin ja alle 1000 robotin hallintaan suositellaan konfiguraatiota, jossa NMS, UMP ja tietokanta toimivat omilla dedikoiduilla palvelimillaan. Kullekin palvelimelle suositellaan 8 – 16 prosessoriydintä ja 16 – 24 GB muistia. NMS tukee Windows Failover Clusteria saatavuuden ja vikasietoisuuden parantamiseksi. [4.]



Kuva 2. Unified Management Portal eli UMP ja hälytysnäkymä.

Hallintakonsoleista UMP ja Admin Console toimivat selaimessa ja Infrastructure manager on Windows-sovellus. UMP:n käyttöliittymä on muokattava ja tarjoaa näkymät häly-

tysten lisäksi Service Level Manageriin (SLM), jota käytetään asiakasraportteihin ja QoS-datan selaamiseen. Kuvassa 2 on esitetty UMP:n hälytysnäkymä. Hälytysten vakavuus ilmaistaan värikoodein, ja hälytysten seulonta esimerkiksi asiakkaan mukaan onnistuu Filter-kentän avulla.

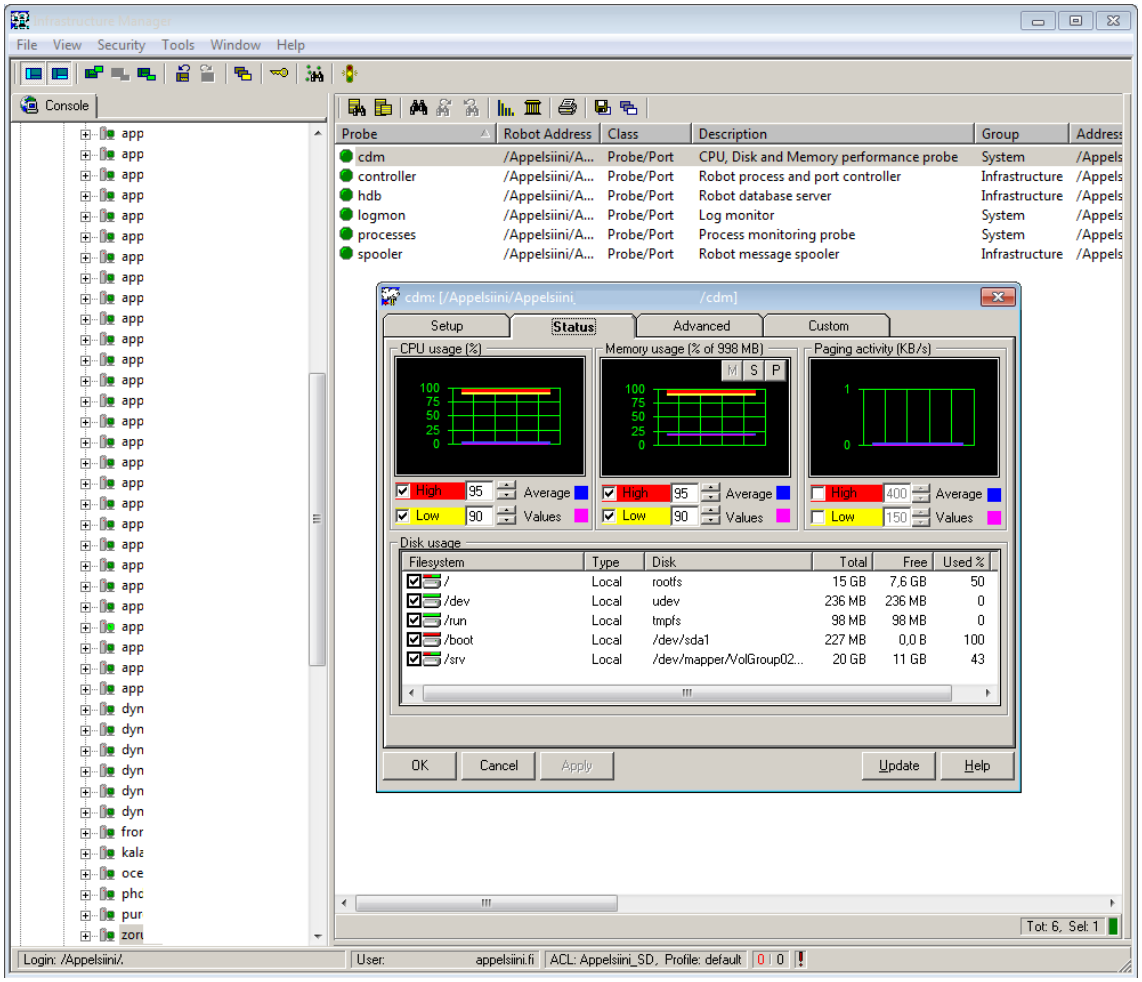
Nimsoftin probe eli anturi on rakenneosa, joka on vastaa tiedon keruusta. Ne jakaantuvat valvonta- ja huoltoprobeihin, joista ensimmäinen kerää saatavuus- ja suorituskykydataa ja jälkimmäinen tarjoaa mahdollisuuden muuttaa tiettyjä asetuksia kohteessaan. Palvelimiin probe asennetaan paikallisesti mutta esimerkiksi verkkolaitteita valvotaan etäprobella, joka on asennettu hubipalvelimelle.

Tyypillisesti kullekin valvontatehtävälle on oma probensa. Esimerkkinä palvelimen perusvalvonta koostuu cdm-, ntevl-, ntperf-, ntservices- ja processes-probeista. Näiden probejen tehtävät ovat:

- Cdm (CPU, disk, memory) valvoo CPU:n, levytilan ja keskusmuistin käyttöä.
- Ntevl seuraa event login merkintöjä.
- Ntperf lukee perfmon dataa.
- Ntservices valvoo Windows-palvelimen palveluiden tilaa.
- Processes valvoo Linux-palvelimen prosesseja.

Etäprobeista usein käytettyjä ovat yksinkertaista ping-valvontaa toteuttava net_connect, verkkosivujen toimintaa testaava url_response, SNMP-trappeja vastaanottava snmptd ja SNMP-kyselyitä lähettävä snmpget.

Kullekin probelle asetetaan raja-arvot tai muut asetukset valvottavan kohteen mukaan. Yksinkertaisissa tapauksissa, kuten ping-valvonnassa, tämä on helppoa, mutta esimerkiksi event login valvonnassa toimivien asetusten haku voi vaatia useampia iteraatiokierroksia. Kuvassa 3 on esitetty näkymä Infrastructure Manageriin, jossa on auki palvelimen CDM-proben konfigurointi-ikkuna. Konfiguraatiossa on asetettu CPU:n ja muistin eriasteisille hälytyksille erilaiset kynnysarvot.



Kuva 3. Infrastructure Manager ja CDM-proben konfigurointi-ikkuna.

Kuhunkin valvonnan kohteeseen asennettava robotti vastaa erilaisten probejen hallinnasta. Robotin asennuksen yhteydessä asennetaan robotin perustoiminnan vaatimat huoltoprobet:

- Controller vastaa robottiin liitettyjen probejen käynnistyksestä ja sammutuksesta.
- Spooler kerää, järjestää ja lähettää edelleen probejen tuottaman datan.
- Hdb vastaa robotin datan säilyttämisestä. Paikallinen säilytys robotin tietokannassa mahdollistaa kynnysarvojen seurannan, trendien analysoinnin ja paremman vikasietoisuuden.

Robotit eivät eroa toisistaan muuten kuin hallitsemiensa probejen osalta. Probeista voidaan koostaa paketteja, joilla voidaan tuottaa valmiita paketteja erityyppisten palveluiden valvontaan. Esimerkiksi Windows-palvelimen perusvalvonnan probet voidaan paketoida ja asentaa Infrastructure Managerissa raahaamalla ne robotin päälle.

Robotti muuttuu hubiksi asentamalla siihen hub-probe. Hubi hallitsee robotteja ja kerää roboteilta tulevan datan välittäen sen eteenpäin sekä säilyttää järjestelmän tietoja kuten nimitauluja. Hubeja on oltava vähintään yksi mutta tyypillisesti niitä on useampia. Ensisijainen hubi (primary hub) luodaan NMS:n asennuksen aikana ja on kuvan 1 mukaisesti yhteydessä tietokantaan. Ensijaisella hubilla on myös NAS-probe, joka vastaa hälytysten lähetyksestä työnohjausjärjestelmään, päivystäjälle ja tarvittaessa kolmansille osapuolille. Toissijaisia hubeja (secondary hub) voi luoda tarvittaessa NMS:n asennuksen jälkeen ja nillä voidaan toteuttaa esimerkiksi verkkoskannausta uusien laitteiden löytämiseksi (device discovery), QoS-datan laskentaa ja robottien ryhmittelyä eri parametrien mukaan. Varahubi (failover hub) on toissijainen hubi, joka ylenee ensisijaiseksi, jos alkuperäiseen ensisijaiseen hubiin ei saada yhteyttä.

Tiedonsiirto järjestelmän osien välillä tapahtuu message busin kautta. Uutta dataa saanut komponentti julkaisee datan väylään, josta muut julkaisijaa kuuntelevat komponentit sen noutavat. Väylässä on myös API, jonka kautta valvontakonfiguraatioita voi muokata. Hubien väliseen tiedonsiirtoon voidaan luoda salattuja SSL-tunneleita, joilla voidaan esimerkiksi yhdistää asiakkaiden verkot internetin yli keskuspalvelimelle.

Nimsoftin tärkeimmät integraatiot ovat Appelsiinin Active Directoryyn ja tuotannonohjausjärjestelmään. AD-integraation kautta hallitaan pääsyä järjestelmään ja tuotannonohjausjärjestelmä on palvelutuotannon keskeinen osa, jossa kaikki tukipyynnöt käsitellään. Tiedot kulkevat itse luodulla probella Nimsoftista Service Now'n tuotannonohjausjärjestelmään, johon hälytyksestä avataan tarvittaessa uusi tiketti. Tikettiin siirtyviä tietoja ovat asiakas, tapahtuma-aika, robotti ja probe. Myös rakenneosa pyritään selvittämään integraation avulla ja liittämään tikettiin. Jos rakenneosa saadaan selvitettyä, voidaan tikettiin liittää myös oikea palvelusopimus, jonka perusteella tiedetään sovitut vasteajat. Hälytyksiä voidaan tuoda tuotannonohjausjärjestelmään myös System Center Operations Manager 2012:sta Nimsoft-integraation avulla.

3.2 Valvontajärjestelmä käyttäjien kannalta

Tähän tutkimukseen haastateltiin vapaamuotoisesti muutamia Appelsiinin ylläpitäjiä, jotka käyttävät valvontaa päivittäisessä työssään. Ylläpitäjien kannalta näkyvin osa valvonnan toimintaa on sen generoimat hälytykset, joita tarkastellaan valvontakonsolista tai hälytysten perusteella luotujen tikettien kautta. Hälytyksistä käy ilmi kohteesta

riippuen vaihtelevasti tietoa, mutta kaikista löytyy ainakin perustiedot kuten hälytyksen lähde (probe ja CI), aikaleima ja hälytyksen toistuvuus. Valvontakonsoli (UMP) on selaimessa toimiva näkymä, jossa hälytyksiä voidaan seuloa ja järjestää halutulla tavalla. Konsoli on ensiarvoisen tärkeä vianetsintätyökalu, koska sillä voidaan nopealla silmäyksellä löytää laitteet tai sovellukset, joissa on häiriöitä ja mahdollisesti suoraan löytää myös häiriöiden juurisyy, esimerkiksi katkennut verkkoyhteys tai kaatunut sovellus.

Haastatteluissa Nimsoft koettiin teknisesti riittävän monipuoliseksi ja toimivaksi järjestelmäksi. Monipuolisuuden haittapuolena tosin on valvonnan konfiguroinnin varsin jyrkkä oppimiskäyrä. Nimsoftin dokumentaatio on onneksi varsin kattava, mutta siihen tutustumiseen ei välttämättä ole riittävästi aikaa palvelutuotannon kiireiden keskellä. Tämän takia valvonnan konfigurointi delegoidaan usein valvontajärjestelmän ylläpitäjälle. Ylläpitäjien toiveissa olikin, että valvonnan käyttöön järjestettäisiin lisäkoulutusta, jolloin mahdollisesti myös vastuuta järjestelmän toiminnasta voitaisiin hajauttaa. Koulutuksen toivottiin myös avaavan paremmin palvelusopimusten sisältöä ja vastuita valvonnan suhteen.

Yksi esille tulleista ongelmista on hälytysten luokittelu. Hälytykset generoidaan Nimsoftissa ja siirretään integraation kautta Service Now'n tuotannonohjausjärjestelmään. Hälytyksen kriittisyys ei kuitenkaan välity oikein tukipyyntöön vaan toistaiseksi manuaalisesti hoidettava lajittelu korjaa vaikutus- ja kiireellisyysparametrit ja ohjaa tiketin oikealle tukiryhmälle.

Nimsoftin käyttöliittymä sai myös kielteistä palautetta. Hälytysten tarkasteluun käytettiin aiemmin erillistä konsolia, jolla hälytysnäkymästä sai kertasilmäyksellä paljon tietoa ja lajittelu ja suodattaminen oli helppoa. Nyt käytössä oleva UMP tarjoaa merkittävästi suppeamman näkymän, ja tarkempien tietojen saamiseksi hälytyksiä joutuu avaamaan yksitellen. Myös asetusten konfigurointi on työlästä, ja usein valvonnan toimintaan saamiseksi pitää tietää tarkasti, mistä jokin yksittäinen asetusrasti löytyy.

Ylläpidon lisäksi tutkimukseen haastateltiin muutamia Appelsiinin palveluista asiakkaille viestiviä henkilöitä. Näissä haastatteluissa kävi ilmi, että asiakkaiden vaatimukset valvonnalle eivät usein ole kovin tarkkoja. Vaatimukset tarkentuvat usein vasta käyttöönottovaiheessa, kun asiakkaan it-henkilöt pääsevät asettamaan vaatimuksia järjestelmälle. Vaikka vaatimukset valvonnalle eivät olisikaan aina erityisen tarkkoja, tiedostetaan valvonnan toiminta myös asiakkaan puolella viimeistään siinä vaiheessa, kun jotakin ha-

joaa tai jokin palvelu on poissa käytöstä. Yleensä tässä vaiheessa halutaan tieto siitä, miten valvonta on hälyttänyt ja miten palveluntuottaja on hälytyksiin reagoinut.

Tulevaisuudessa odotettavat haasteet liittyvät suurelta osin Appelsiinin nopeaan kasvuun. Asiakkaiden määrän ja koon kasvaessa myös valvottavien kohteiden määrä kasvaa nopeasti, mikä asettaa vaatimukset valvontajärjestelmän skaalautuvuudelle. Tällä hetkellä valvonnan piirissä on jo tuhansia laitteita ja palveluita. Suurempien asiakkuuksien mukana palveluun ja siten myös valvontaan tuodaan mahdollisesti myös suurempia ja haastavampia järjestelmiä, kuten SAP. IT-alan trendi palveluiden pilveen siirtymisessä on nähtävissä valvontatuotteiden markkinointimateriaaleissa, mutta sillä ei ainakaan lyhyellä tähtäimellä ole vaikutusta Appelsiinin valvontatuotteen valintaan, koska pilvipalvelut tuotetaan konsernin toisessa yksikössä.

4 Valvontajärjestelmän vaatimusmäärittely

Vaatimusmäärittely suoritettiin haastattelemalla Appelsiinin Nimsoft-ylläpitäjää sekä muutamia asiantuntijoita, joilla on vankan kokemuksen lisäksi hyvä tietämys Appelsiinin asiakkaiden arkkitehtuureista. Lisäksi asiakkaan näkökulmaa haluttiin tuoda esille haastattelemalla myynnin ja kehityksen tehtävissä toimivia henkilöitä, jotka ovat suorassa asiakaskontaktissa.

Teknisesti valvontajärjestelmän valinnan rajaavimpia tekijöitä on se, että järjestelmän on oltava kaupallinen. Avoimen lähdekoodin järjestelmän käytölle ei ole esteitä, mutta tuotteen tuen on oltava kunnossa ja saatavilla lyhyellä vasteajalla. Tuotteen elinkaarta kannattaa myös koettaa arvioida, sillä kyseessä on liiketoimintakriittinen järjestelmä.

Järjestelmä halutaan Appelsiinin omaan kapasiteettiin ja ylläpitoon, joten SaaS-ratkaisut rajautuvat pois. Fyysisellä laitteella (appliance) toteutetut järjestelmät jätetään myös huomiotta. Arkkitehtuuritasolla järjestelmän halutaan olevan hajautettu siten, että asiakkaiden laitteissa olevia valvontakomponentteja voidaan hallita keskuspalvelimelta ja valvontatiedot kootaan keskuspalvelimelle. Tiedonsiirto kohteesta keskuspalvelimelle tulee onnistua myös internetin yli salattuna. Järjestelmien välistä tiedonsiirtoa ja muita integraatioita varten tarvitaan API eli ohjelmointirajapinta, jonka kautta tulee onnistua myös valvontaparametrien käsittely. Järjestelmässä tulee olla myös discovery-toiminta, joka hakee verkosta uusia laitteita.

Datan keruun halutaan toimivan agenttien avulla ja tarvittaessa myös agentittomasti. Agenttien hallinnan halutaan toimivan keskitetysti asennusten (push-asennus) ja valvonta-asetusten tarkastamisen osalta. Datan varastointi on tapahduttava tietokantaan, sillä varastoitavan datan määrä ja hakuominaisuuksien tarve sulkee pois flat file -ratkaisut. Appelsiinin tukemat ratkaisut tietokannoissa ovat Microsoft SQL Server ja MySQL, mahdollisesti myös PostgreSQL.

Palvelutuotannon erityispiirteenä on se, että saman valvontajärjestelmän on palveltava kaikkien asiakasorganisaatioiden verkkoja (multitenancy). Päällekkäisyyksiä voi esiintyä lähes kaikissa resursseissa kuten IP-osoitteissa ja käyttäjätunnuksissa, joten asiakasorganisaatiot on voitava erottaa toisistaan loogisesti ja helposti.

Asiakkuuksien erottamisen tulee heijastua myös käyttöliittymään, jonka halutaan olevan käyttäjäkohtaisesti mukautettava. Asiakkaille on voitava julkaista portaali, josta näkee ainoastaan kyseiseen asiakkaaseen liittyvää tietoa. Raportointiominaisuuksista tarvitaan ainakin SLA- ja trendiraportointi.

Useat valvontatuotteet keskittyvät pääasiassa verkon ja verkkolaitteiden valvontaan, mutta Appelsiinin oleellisimpia erityispiirteitä valvonnan kannalta on se, että valvonta keskittyy enemmän palvelimiin ja sovelluksiin. Käytettävän valvontajärjestelmän onkin tuettava yleisimpiä palvelinten käyttöjärjestelmiä:

- Windows Server (2000 ja uudemmat)
- Linux-distribuutiot, esimerkiksi Ubuntu ja CentOS
- Unix-variantit kuten Solaris ja FreeBSD.

Työpöytäkäyttöjärjestelmien ja eksoottisempien palvelintuotteiden, kuten OpenVMS:n tuki lasketaan tietenkin hyödylliseksi lisäksi.

Sovellusten osalta valvontaan halutaan varsinkin yleisimmät Microsoftin palvelinsovellukset Exchange, IIS, SQL Server ja Lync Server. Appelsiinin Microsoft-partneruuden myötä uudet versiot käyttöjärjestelmistä ja sovelluksista otetaan tuotantoon aikaisessa vaiheessa, joten valvontajärjestelmän kehityksen olisi syytä seurata Microsoftin julkaisuja nopealla tahdilla. Myös Powershell-tuki osoittautunee jatkossa entistä tärkeämmäksi Microsoftin siirtäessä sen taakse yhä enemmän toimintoja. Toisaalta tuotannos-

sa on myös vanhempia järjestelmiä kuten Windows 2000, joten ajassa taaksepäin ulottuva tukikin on tarpeen.

Useissa asiakasympäristöissä verkon ja verkkolaitteet toimittaa niihin erikoistunut toimittaja, joten Appelsiinin valvontavastuut rajoittuvat lähinnä laitteiden ping-valvontaan. Appelsiinin vastuulla on kuitenkin jonkin verran verkon aktiivilaitteita oman verkon lisäksi, joten verkonvalvontaominaisuuksia ei voida kokonaan sivuuttaa. SNMP-valvonnan (trap, get) lisäksi olisikin toivottavaa, että valvontatuotteesta löytyisi tuki ainakin tunnetuimpien valmistajien laitteille valmiiksi konfiguroitujen laitepohjien (template) muodossa.

Merkittävä tekijä soveltuvan tuotteen valinnassa on myös asennuksen ja ylläpidon vaatima työmäärä. Jos tuotteen käyttö ja konfigurointi on helppoa, sen ylläpitoon ei välttämättä tarvita dedikoitua asiantuntijaa. Lisäksi konfiguroinnin helppous ja nopeus säästävät jokaisen ylläpidossa työskentelevän työaikaa, joskus jopa merkittävästi.

5 Markkinakartoitus

Markkinoilla on runsaasti erilaisia valvontajärjestelmiä, joiden ominaisuudet vaihtelevat laidasta laitaan. Osa valvoo ainoastaan verkkolaitteita, osa myös verkossa toimivia sovelluksia. Ilmaisia, avoimen lähdekoodin sovelluksia on myös saatavilla. Joistakin tuotteista on saatavilla sekä rajoitetumpi ilmaisversio, että kaikki tuotteen toiminnot sisältävä maksullinen versio.

Markkinatutkimusyhtiö IDC:n arvion mukaan vuoden 2012 markkinajohtaja verkonvalvontasovellusten ja -laitteiden osalta oli Netscout, jonka tuotteet keskittyvät pääosin verkkoliikenteen valvontaan [5]. Edellisenä vuonna markkinajohtaja oli CA Technologies, joka tarjoaa edellä esitellyn Nimsoftin lisäksi useita muita valvontatuotteita [6]. Muita tunnettuja suuryrityksiä markkinoilla ovat HP, IBM, Fujitsu ja BMC.

Kaikkien markkinoilla olevien tuotteiden kattava vertailu ei ole tämän kartoituksen puitteissa mahdollista, joten tarkemmin vertailtavat tuotteet valittiin tutustumalla Googlen antamiin hakutuloksiin, esimerkiksi hakutermeillä ”network management” ja ”verkonvalvonta”, Wikipedian listaukseen verkonvalvontajärjestelmistä [7] ja keskustelemalla aiheesta kollegoiden kanssa.

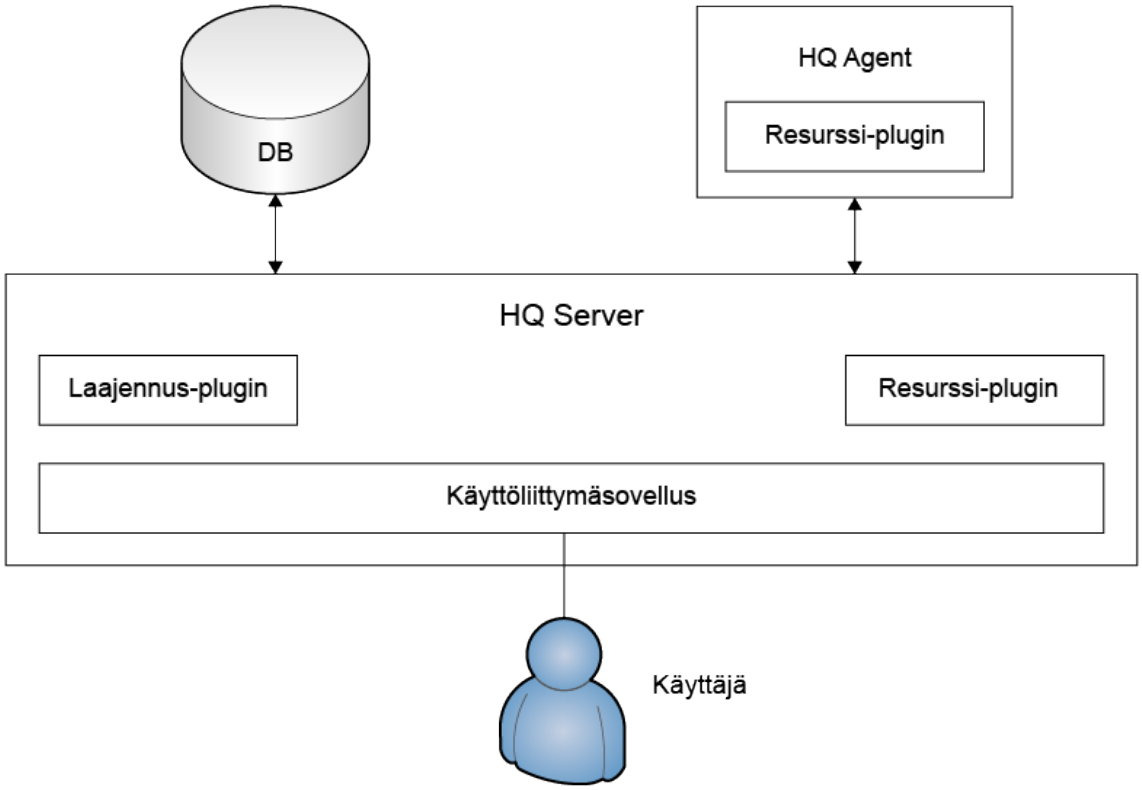
Edellä mainituin perustein Nimsoftin vaihtoehtoina tarkasteltavien valvontatuotteiden lista supistui merkittävästi. Appelsiinin kannalta mielenkiintoisimpia valvontatuotteita Nimsoftin lisäksi ovat vCenter Hyperic, Pandora FMS ja ScienceLogic EM7.

5.1 vCenter Hyperic

Hypericin juuret ovat Java-sovellusten ja -ympäristöjen valvonnassa. SpringSource osti Hypericin keväällä 2009 ja myöhemmin samana vuonna VMWare osti puolestaan SpringSourcen. Hypericin tuorein kaupallinen versio on nimeltään vCenter Hyperic ja ilmaisversio kulkee nimellä Hyperic HQ. Maksullinen tuote on ollut aiemmin nimeltään myös Hyperic HQ Enterprise sekä vFabric Hyperic, joihin molempiin löytyy vielä useita viittauksia valmistajan verkkosivulta. [8 – 10.]

Hypericin painopiste on sovellus- ja sovelluspalvelinvalvonnassa, johon se tarjoaa varsin kattavat työkalut. Lisäksi omistajanvaihdos on tukenut voimakkaasti VMWare-integraation kehitystä. Tärkeimmät Hypericin tukemat valvottavat teknologiat kategorioittain ovat:

- Käyttöjärjestelmät: Windows Server (2003 -), Linux, Unix, FreeBSD, AIX, HP-UX, Solaris ja Mac OS X.
- Tallennus: Netapp.
- Verkot: Kytkimet, reitittimet ja palomuurit SNMP- ja ICMP-protokollien avulla. Cisco IOS, PIXOS ja CATOS-käyttöjärjestelmät.
- Virtualisointi: VMWare ja XenServer.
- Tietokannat: Microsoft SQL Server, MySQL, PostgreSQL, IBM DB2, Oracle, Sybase ja Gemfire.
- Sovellukset: Active Directory, Exchange, IIS, Apache, Tomcat, Citrix, JBoss, JRun ja .Net Runtime.



Kuva 4. Hypericin arkkitehtuurin pääkomponentit.

Hypericin arkkitehtuuri on esitetty kuvassa 4 ja muistuttaa Nimsoftia: Tärkeimmät komponentit ovat keskuspalvelin HQ Server, agentit, tietokanta ja selainpohjainen käyttöliittymä Hyperic Portal. Paikallisesti valvottaviin kohteisiin asennetaan agentti, joka aluksi skannaa kohteen sovelluksineen. Agentilla valvotaan erilaisia suorituskyvyn parametreja sekä kohteen logeja ja tapahtumia. Agentilla voi myös kontrolloida sovelluspalvelimia. Agenttien keräämä data lähetetään keskuspalvelimelle, joka eskaloi hälytykset eteenpäin ja tallentaa datan PostgreSQL-tietokantaan. Keskuspalvelin sisältää oman JBoss-sovelluspalvelimensa.

Hypericin autodiscover eli verkon laitteiden ja palveluiden automaattinen haku luo inventaarion löydetyistä laitteista ja niiden välisistä relaatioista. Inventaariomalli lajittelee autodiscoverin löytämät resurssit hierarkkisesti yksittäisiin inventaariotyyppeihin

- Alusta (platform) on yleensä laite, jossa on käyttöjärjestelmä.
- Palvelin (server) on ohjelmistotuote, jota ajetaan käyttöjärjestelmän päällä kuten tietokantainstanssi tai sovelluspalvelin.
- Palvelu (service) on olennainen osa alustaa tai palvelinta kuten tiedostojako tai tietokannan taulu.

Ryhmä (group) ja sovellus (application) ovat monikollisia inventaariotyyppejä, joiden avulla resursseja voidaan ryhmitellä. Kukin yksittäinen resurssi edustaa myös resurssityyppiä, joka identifioi sen tarkoituksen tarkemmin. Esimerkiksi Windows-palvelimen resurssityyppi on ”Win32” ja Linux-palvelimen ”Linux”. Käyttäjä voi lisäksi määritellä sovellus-resursseja. Samanlaisia resursseja sisältäviä ryhmiä voidaan käsitellä yhtenä instanssina. Esimerkiksi uudelleenkäynnistyskomento voidaan antaa useiden resurssien sijasta ryhmälle. [11.]

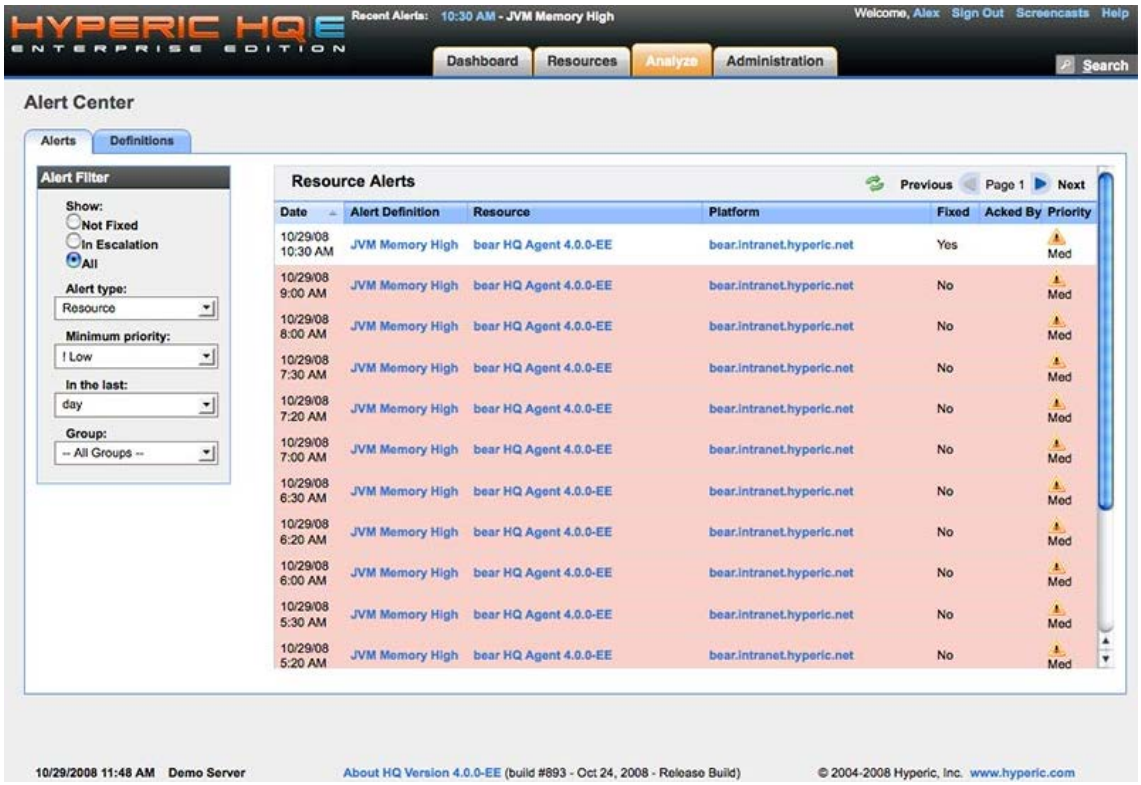
Hypericin toiminnallisuutta voi laajentaa kahdenlaisilla plugineilla. Agentit käyttävät resurssi-plugineja resurssien etsintään, valvontaan ja hallintaan. Laajennus-pluginit ovat käyttäjien kehittämiä laajennuksia muun muassa käyttöliittymään, prosessien automatisointiin ja muihin valvontajärjestelmiin integroimiseen.

Sovelluspalvelin voidaan asentaa Red Hat- tai CentOS-alustalle tai käyttää valmista virtuaalikonetta (vApp). Viimeksi mainittu vaihtoehto on mielenkiintoinen, koska se säästää järjestelmän asennuksen vaatimaa aikaa ja vaivaa. Keskuspalvelin ja erillisessä virtuaalikoneessa toimiva tietokanta ovat käyttökunnossa helposti VMWareen tuomalla.

Kuva 5. Hypericin käyttöliittymän dashboard-näkymä [1].

Sovellus- ja tietokantapalvelimet suositellaan asennettavaksi eri palvelimille, kun valvonnassa on yli 100 alustaa. Kun valvonnassa on 500 – 2000 alustaa tai yli 30 000 resurssia, laitevaatimuksena on sovelluspalvelimelle 6 CPU:ta ja 12 GB muistia ja tietokantapalvelimelle 8 CPU:ta ja 16 GB muistia. Hyperic tukee sovelluspalvelimen kahdennusta klusteroimalla, mutta klusteritoteutus vaatii erillisen kuormanjakolaitteen käyttöä.

Kuvassa 5 on esitetty Hypericin käyttöliittymän dashboard-näkymä. Selainpohjainen käyttöliittymä on toteutettu HTML5:llä ja on käyttäjäkohtaisesti muokattavissa. Etusivulla esitetään esimerkiksi tuoreimmat inventaariomuutokset ja hälytykset. Portaalin kautta voidaan hallita myös valvonta-asetuksia ja inventaariota sekä luoda raportteja. Raportointi kattaa muun muassa SLA-raportit, mutta vaikuttaa ainakin oletuskonfiguraatiossaan vaatimattomalta. Omia raportteja voi tuottaa JRXML-kielellä ja SQL-kyselyillä. Myös kuvassa 6 esitetty Hypericin hälytysnäkymä välittää melko vähän tietoa ja vaikuttaa käyttömahdollisuuksiltaan vajaalta.



Kuva 6. Hypericin hälytysnäkymä [12].

Pääsynhallintaan voidaan käyttää Hypericin omaa kantaa tai LDAP-hakemistoa. Käyttäjille voidaan luoda ryhmiä ja käyttöoikeuksia voidaan niputtaa erilaisiksi rooleiksi.

Roolit kiinnitetään ryhmiin ja niiden kautta voidaan säätää myös asiakkaille annettavat näkymät dataan [13].

Hypericin API on nimeltään HQApi ja tarjoaa suoran pääsyn Hyperic Serverin toimintoihin ja dataan ohi käyttöliittymän. API:in pääsee käsiksi ohjelmallisesti Java-metodeilla tai RESTful web-palvelun kautta. API:in pääsee myös erillisellä komentorivityökalulla, jolla onnistuu myös skriptaaminen. API:n avulla voi automatisoida tapahtumia, tehdä suuria datan päivityksiä (bulk data) ja luoda integraatioita toisiin järjestelmiin.

Hypericin perusvalvonnan konfigurointi on dokumenttien perusteella helppoa. Agentin asennuksen jälkeen se löytää asennusalustansa resurssit ja lisää ne tietokantaan. valvonta-asetuksille voi luoda asetuspohjia eli templateja, joiden avulla tarkemmat asetukset saa helposti kohdalleen. Perusasennus kattaa tyypillisimmät valvontatarpeet varsin hyvin ja plugineja löytyy paitsi Microsoftin sovelluksille myös verkkolaitteille. Hälytyksen voi konfiguroida kynnykseksi paitsi staattisen raja-arvon, myös poikkeaman järjestelmän laskemasta baseline-arvosta. Hälytyksille voi asettaa myös loogisia ehtoja.

Hypericin vahvuudet ovat:

- VMWare-integraatio
- Erilaisten sovelluspalvelinten valvonta
- Integraatio ilmaisiin Nagiokseen ja OpenNMS:ään
- Datan ekstrapolointi ja baselinen määritys.

Hypericin heikkoudet ovat:

- Uusin versio tukee tietokantana vain PostgreSQL:aa.
- Keskittyy enemmän organisaation oman verkon valvontaan kuin palvelutoimittajan monen asiakkaan ympäristöön.
- Dokumentaatiossa on puutteita ja verkkosivuilla lukuisia ongelmia versiomuutosten jäljiltä.
- Käyttöliittymä on tyylikäs, mutta ominaisuuksiltaan vaatimaton.

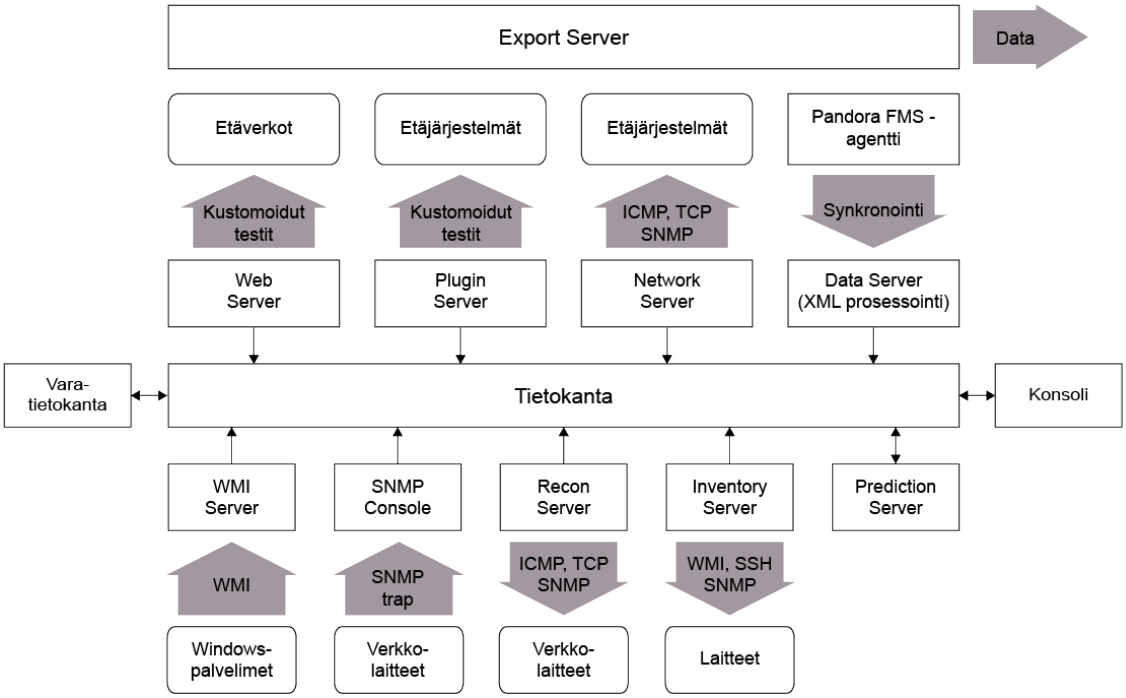
5.2 Pandora FMS

Pandora FMS on avoimen lähdekoodin valvontajärjestelmä, jolle Artica ST myy vuosimaksulla tukipalvelut sisältäviä enterprise-lisenssejä, jonka hinta määräytyy valvottavien laitteiden määrän mukaan [14].

Pandora tarjoaa varsin kattavan tuen valvottaville järjestelmille. Järjestelmä tukee myös yleisimpiä palvelinalustoja ja verkkolaitteita sekä Microsoftin järjestelmiä mukaan lukien:

- käyttöjärjestelmät: Windows Server (2000 -), Linux, Unix, FreeBSD, AIX, HP/UX, Solaris ja Mac OS X
- tallennus: Netapp
- verkot: kytkimet, reitittimet ja palomuurit SNMP-, ICMP-, TCP-, UDP- ja DNS-protokollien avulla
- virtualisointi: VMWare, XenServer, Hyper-V, RHEV ja Amazon AWS
- tietokannat: Microsoft SQL Server, MySQL, PostgreSQL, IBM DB2, Oracle ja Informix
- sovellukset: Active Directory, Exchange, Sharepoint, IIS, Apache, Lotus Notes Tomcat, Citrix, JBoss ja SAP.

Arkkitehtuuriltaan Pandora on hajautettu, modulaarinen ja poikkeaa jonkin verran aiemmin esitetyistä. Kuvassa 7 on esitetty arkkitehtuurimalli, jossa keskeisin osa on tietokannalla. Valvontadataa keräävät sekä agentit että erityyppiset palvelimet. Selainpohjainen käyttöliittymä toimii konsolissa. [15.]



Kuva 7. Pandora FMS:n arkkitehtuuri.

Tällä hetkellä ainoa tuetttu tietokanta-alusta on MySQL. Kannan huoltotoimenpiteet on pitkälti automatisoitu, ja ne ovat varsin aggressiivisia. Oletusasetuksilla kaikki 30 päivää vanhempi data pakataan ja 90 päivää vanhempi data poistetaan kannasta kokonaan.

Valvontadataa kerätään agenteilla, jotka jakautuvat loogisiin agentteihin, ohjelmistopohjaisiin eli softa-agentteihin ja laitepohjaisiin eli rauta-agentteihin. Softa-agentti on kohdelaitteelle asentuva ohjelma, joka kerää tietoa paikallisesta järjestelmästä. Agentin konfigurointi tapahtuu konfiguraatiotiedostoa muuttamalla tai hallintakonsolista. Kukin kerätty datatyyppi muodostaa moduulin, joka voidaan lukea Pandoran web-konsolissa toimivalla loogisella agentilla. Datasta voidaan myös muodostaa XML-muotoisia paketteja, jotka lähetetään datapalvelimille FTP:llä tai salattuna SSH- tai Tentacle-protokollalla. Pakettien lähetysväli on oletuksena 300 sekuntia eikä alle 100 sekunnin lähetysväliä suositella [16]. Rauta-agentti on HW groupin valmistama laite, joka valvoo ympäristön tilaa mitaten muun muassa lämpötilaa ja ilmankosteutta.

Vaikeapääsyisiä verkkoja voi valvoa satelliitti- ja drone-agenteilla, jotka toimivat välityspalvelimina verkkojen välillä. Mielenkiintoinen lisä ovat myös Android- ja Windows Phone-mobiilikäyttöjärjestelmiin asentuvat agentit, joilla voi hakea muun muassa laitteen GPS-koordinaatit.

Dataa kerätään myös erityyppisillä palvelimilla, joita on kaikkiaan 12 erilaista ja jotka ovat suoraan yhteydessä tietokantaan. Palvelinprosesseja voidaan tarvittaessa ajaa myös samalla palvelimella. Palvelinten toimintaan kuuluu myös hälytysten generointi. Palvelintyyppejä ovat muun muassa:

- Datapalvelin kuuntelee softa-agenttien lähettämää liikennettä ja muokkaa datan sopivaan muotoon kantaan tallennusta varten.
- Network-palvelin valvoo verkkopalveluita ICMP-protokollalla ja verkkolaitteita SNMP-protokollalla.
- SNMP-konsoli vastaanottaa verkkolaitteiden SNMP trappeja.
- Web-palvelin valvoo verkkosivujen toimintaa testaamalla esimerkiksi verkkolomakkeen täyttöä tai sivulla olevan elementin ”klikkaamista”. Toiminta vahvistetaan tutkimalla saatua paluuarvoa kuten tiettyä tekstinpätkää. Vasteajan valvonta on myös mahdollista.
- WMI-palvelin tekee Windows-palvelinten etävalvontaa WMI-protokollalla.
- Recon-palvelin etsii uusia järjestelmiä ja luo topologiakarttoja.
- Plugin-palvelimella voi ajaa kustomoituja valvontatyökaluja. Pluginien kehittämisessä tuetut kielet ovat VBScript, Powershell, Perl, Python ja shellscript.
- Prediction-palvelin analysoi mittausdataa ja pyrkii ennustamaan tulevaa kehitystä sekä tunnistamaan poikkeamia datassa.
- Export-palvelin replikoi mittausdataa toiseen Pandora-instanssiin valvonnan keskittämistä varten.

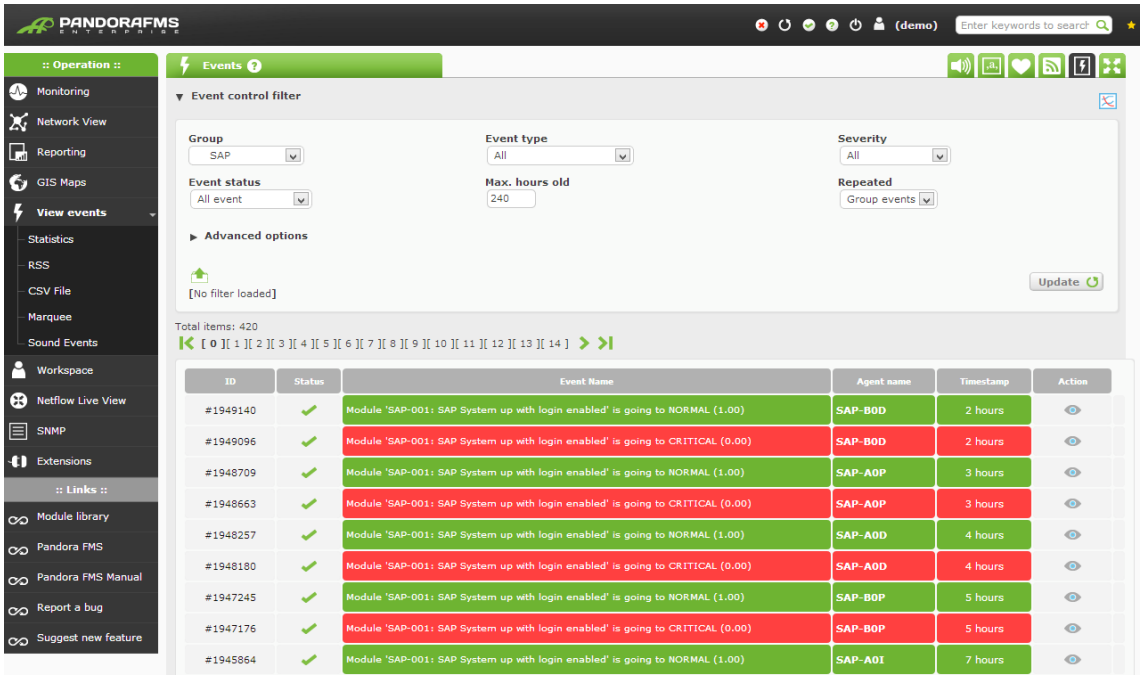
Pandoran sovelluspalvelimet toimivat Linux-, BSD- tai Solaris-alustalla ja käyttävät Apachea, PHP5:ttä ja Perliä. Pandoran saatavuutta voidaan parantaa kahdentamalla palvelimia aktiivi-passiivi-pareiksi. Suorituskykyä ja kapasiteettia voidaan puolestaan parantaa lisäämällä kokonaisia Pandora-instansseja, joiden keskitetty hallinta onnistuu Metaconsole-työkalulla. Yhden palvelimen toteutuksella voi hallita noin 1000 – 1500 agenttia. Tuotantokäytössä Pandoraa ei suositella asennettavaksi virtualisoidulle alustalle. [16.]

Selainpohjainen käyttöliittymä perustuu HTML5:een, ja sen ulkonäkö on muokattavissa ryhmä- ja käyttäjäkohtaisesti widgeteillä. Käyttöliittymän kautta voi tarkastella muun muassa valvontadataa, hälytyksiä, konfiguraatioita ja erityyppisiä raportteja. Mielenkiintoisena lisäominaisuutena käyttöliittymä tarjoaa myös selaimessa toteutetut Telnet-, SSH- ja VNC-konsolit järjestelmien keskitettyyn etähallintaan. Käyttöliittymässä on

myös API (Rest) kolmannen osapuolen tuotteiden integraatiolle. GUI:n lisäksi Pandora tarjoaa käyttöliittymän myös komentorivin kautta. Tätä kautta voidaan hallita monipuolisesti muun muassa agenttien toimintaa. Myös komentorivi mahdollistaa integraation kolmannen osapuolen järjestelmiin skriptien kautta.

Raportointiominaisuudet kattavat SLA-raportit, trendit, inventaariot ja verkkotopologiat. Raportit voi tuottaa muokattavalle pohjalle ja tarvittaessa luoda niistä html-, pdf- tai xml-tiedostoja, jotka voi välittää ajastetusti eteenpäin sähköpostilla. SLA-raportoinnissa voidaan valita kullekin parametrille hyväksytyt raja-arvot ja luoda raportti korkeintaan puolen vuoden takaisesta datasta. Raportteja on mahdollista luoda myös ITIL-metriikan pohjalta. [17.]

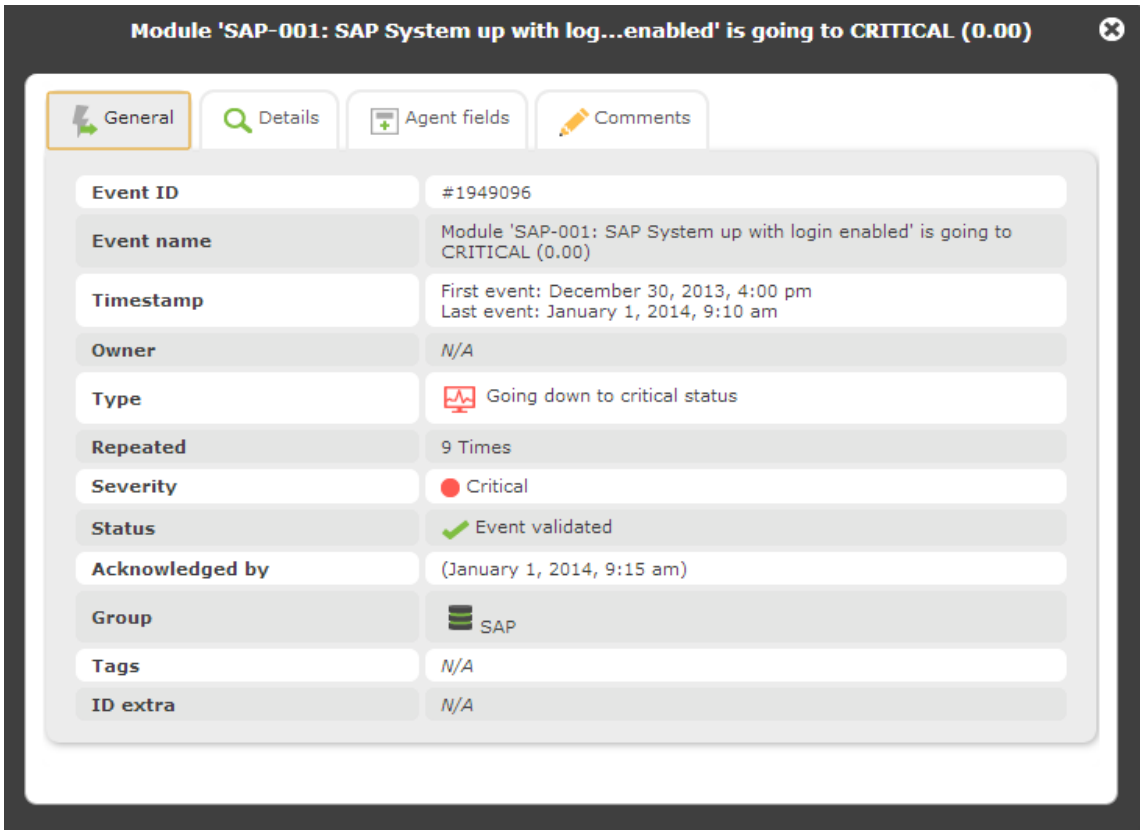
Oikeudet eri näkymiin ja toimintoihin säädetään hienojakoisesti käyttäjätileillä, profiileilla ja ryhmillä. Valvottavat kohteet liitetään ryhmiin, joihin annetaan ryhmäkohtaiset oikeudet. Käyttäjätilit saavat oikeudet ryhmäjäsenyyksien kautta. Käyttäjätilien autentikointi voidaan toteuttaa Active Directoryn kautta.



Kuva 8. Pandora FMS:n tapahtumanäkymä.

Käyttöliittymää pääsee koekäyttämään Pandoran verkkosivujen kautta [18]. Kokeilun perusteella käyttöliittymä on toimiva ainakin yhden organisaation verkon hallintaan. Kuvassa 8 on näkyvissä demosta otettu ruutukaappaus, jossa näkyy suodatettu tapah-

tumanäkymä. Kuvassa 9 näkyvät tapahtuman tarkemmat tiedot. Käyttöliittymä tuntuu toimivan varsin loogisesti, mutta on pikemminkin tyylikäs kuin informatiivinen. Demon perusteella ei valitettavasti voinut arvioida, miten Pandora soveltuu palvelutuotantoon tai Microsoftin tuotteiden valvontaan.



Kuva 9. Pandora FMS:n tapahtuman tietojen näkymä.

Pandora FMS:n vahvuudet ovat:

- asiakkuuksien erottelu (multi-tenancy)
- monipuolinen valvonta laitteille ja sovelluksille
- hyvä skaalautuvuus palvelimia lisäämällä.

Pandora FMS:n heikkoudet ovat:

- Järjestelmä ei ole suunniteltu reaaliaikaiseksi.
- Dokumentaatio on aihepiiriltään kattava, mutta kieliasu on monin paikoin niin heikko, että ymmärrettävyys kärsii.

5.3 ScienceLogic EM7

ScienceLogicin EM7 on CentOS-käyttöjärjestelmän päällä toimiva virtuaalinen tai fyysinen laite. Laite sisältää kaikki tuotteen ominaisuudet, ja lisensointimaksun suuruus riippuu valvottavien laitteiden määrästä. EM7 on saanut muutamia hyviä arvosteluja, mutta sen dokumentaatio on valitettavasti saatavilla vain rekisteröityneille asiakkaille. EM7 otettiin kuitenkin mukaan vertailuun, koska siitä on saatavilla perustiedot valmistajan verkkosivuilta ja muutamien arvostelujen kautta. Toisaalta palvelutuotantoon sopivia valvontajärjestelmiä on tarjolla vain muutamia, joten lupaavaa tuotetta ei haluttu sivuuttaa. [19; 20.]

EM7:n tuettujen teknologioiden lista on ainakin valmistajan verkkosivun mukaan hieman suppeampi kuin kilpailijoilla. Toiminnallisuuden laajentamiseen on kuitenkin tarjolla lisäosia, joita valmistaja kutsuu nimellä PowerApps. Lisäosien kehitykseen on tarjolla graafinen työkalu. Tuettuja järjestelmiä ovat ainakin [21]:

- käyttöjärjestelmät: Windows, Linux, Unix, FreeBSD, AIX, HP/UX ja Mac OS X.
- verkot: kytkimet, reitittimet ja palomuurit SNMP-, ICMP-, TCP-, UDP- ja DNS-protokollien avulla.
- virtualisointi: VMWare, XenServer ja Hyper-V.
- tietokannat: Microsoft SQL Server, MySQL, PostgreSQL ja Oracle.
- sovellukset: Active Directory, Exchange, Sharepoint, IIS, Apache, Tomcat ja Citrix.
- laitevalvonta: Dell OpenManage, HP Insight, IBM Director ja Cisco UCS.

Perusmuodossaan EM7:n toiminnot on keskitetty yhteen laitteeseen, joka sisältää myös tietokantainstanssin. Tietokanta-alustana ScienceLogic käyttää MySQL:ää. Sama laite siis huolehtii verkon laitteiden etsimisestä, valvontadatan keruusta etänä tai agenttien avulla, datan tallennuksesta sekä tietojen esittämisestä käyttöliittymän kautta. Laitteita lisäämällä voidaan parantaa järjestelmän kapasiteettia ja vikasietoisuutta ja niitä voidaan sijoittaa myös etäverkkoihin datan kerääjiksi. Laitteita lisäämällä niiden rooleja voidaan myös eriyttää esimerkiksi dedikoimalla laitteita tietokantakäyttöön. [22; 23.]

Kuva 10. ScieceLogic EM7:n dashboard-näkymä [2].

Kuvassa 10 on esitetty ScienceLogicin selainpohjainen käyttöliittymä, joka on toteutettu HTML5:llä ja Flashilla. Käyttöliittymä on muokattavissa käyttäjä- ja ryhmäkohtaisesti. Pääsynhallinta tapahtuu paikallisten tai AD/LDAP:lla haettavien käyttäjäryhmien kautta ja ryhmille voidaan asettaa erilaisia oikeuksia näytettävään dataan. Valvonnan lisäksi EM7:n toiminnallisuus kattaa myös tiketöintijärjestelmän asiakastuelle sekä laskutustoimintoja palvelunhallinnalle. Nämä sisäänrakennetut järjestelmät herättävät kysymyksen siitä, miten hyvin vastaavien ulkoisten järjestelmien integraatio on otettu huomioon. Integraatiot toteutetaan ScienceLogicin RESTful API:n avulla. [24;25.]

ScienceLogic EM7:n vahvuudet ovat

- asiakkuuksien erottelu (multi-tenancy)
- nopea käyttöönotto.

ScienceLogic EM7:n heikkoudet ovat

- ensisijaisesti laitepohjainen ratkaisu
- tietokanta on integroitu sovelluspalvelimeen
- ei tietoa käyttäjä/kehittäjä foorumista
- nojaa vahvasti agentittomaan valvontaan
- teknisten tietojen johdonmukainen pimittäminen on epäilyttävää.

6 Yhteenveto

Nopealla silmäyksellä valvontatuotteiden valikoima vaikuttaa suorastaan ylitsepursuavalta. Esimerkiksi Wikipedian verkonvalvontajärjestelmien vertailutaulukossa [3] on 61 tuotetta, ja taulukon tuotteista lähes kolmasosa sisältää kaikki taulukossa eritellyt ominaisuudet. Taulukkoa voi internetin resurssien huolellisen läpikäymisen perusteella pitää varsin luotettavana katsauksena valvontamarkkinoiden nykytilanteeseen.

Yhden suuren yrityksen infrastruktuurin valvontaan löytyy vielä useita enterprise-tyyppisiä tuotteita, mutta useimmat niistäkin karsiutuvat pois, kun haetaan järjestelmää, joka toimii palvelutuottajan ympäristössä. Palvelutuotannon moniasiakasympäristö on haastava päällekkäisten IP-osoitteiden ja laitenimien viidakko, jossa valvontatuotteen tietoturva- ja pääsynhallintaominaisuudet korostuvat ja kaikkia verkkoon liitettäviä laitteita valvova ohjelmisto pitäisi toteuttaa helpolla mutta monipuolisella käyttöliittymällä. Ei siis ole ihmekään, että moni valvontatuote karsiutui vertailusta pois.

Zenoss ja Solarwinds olivat muuten vakuuttavia ja monipuolisia järjestelmiä, mutta niiden täysin agentiton toimintaperiaate ei sovellu Appelsiinin käyttöön. Nagios ja siihen pohjautuvat tuotteet, esimerkiksi Op5 Monitor, jätettiin myös vertailun ulkopuolelle, niiden Linux/Unix-keskeisyyden ja työlään ylläpidon vuoksi. Tämä oli harmillista, sillä Nagios vaikutti joustavalta ja suurempiinkin ympäristöihin skaalautuvalta järjestelmältä. HP:n ja IBM:n tuotteet jätettiin myös tarkastelun ulkopuolelle.

Nyt käytössä olevalle Nimsoftille jäi siis kolme kilpailijaa, jotka pääosin täyttävät luvussa neljä esitellyt kriteerit. Nimsoft on toiminut varsin luotettavasti eikä sen toiminnallisuudessa Appelsiinin ympäristössä ole ollut merkittäviä puutteita, joten se asettaa hyvän vertailukohdan kilpailijoilleen. Ylläpitäjien kommentit ovat kertoneet lähinnä puutteista käyttöliittymässä, joka ilmenee muun muassa hankalahkona konfigurointina.

Taulukossa 1 on esitetty kolmen Nimsoftin verrokeiksi valittujen järjestelmien tärkeimpien ominaisuuksien arviointi suhteessa Nimsoftiin. Taulukko on jaettu alustan ominaisuuksiin ja valvontaominaisuuksiin. Taulukosta on jo nähtävissä suuntaa-antavasti vertailun lopputulos, mutta seuraavassa eritellään vielä järjestelmien eroja hieman tarkemmin.

Taulukko 1. Vertailtujen valvontajärjestelmien ominaisuudet suhteessa Nimsoftiin. Miinusmerkki tarkoittaa heikompaa, +/- yhtähyvää ja plusmerkki parempaa. Kahdella merkillä ilmaistaan huomattavasti heikompaa tai parempaa.

	vCenter Hyperic	Pandora FMS	ScienceLogic EM7
Asennus ja alusta			
Alustavaihtoehdot	--	-	--
Tietokantavaihtoehdot	--	-	-
Skaalautuvuus ja HA	-	+/-	+/-
Dokumentaatio	+/-	+/-	Ei tiedossa
Ominaisuudet			
Palvelinvalvonta	-	+/-	+/-
Sovellusvalvonta	+	+/-	+/-
Verkonvalvonta	+	+/-	+/-
Käyttöliittymä: Hälytysnäkymä	-	-	++
Käyttöliittymä: Konfigurointi	+/-	-	+
Käyttöliittymä: Raportointi	-	-	+
Multitenancy	-	+/-	+/-
API ja integraatiot	-	+/-	-

Teknisistä tekijöistä ehkä olennaisin on, mitä kaikkea kullakin tuotteella voidaan valvoa. Standardoidut verkonvalvontaprotokollat löytyvät kaikista tuotteista, ja palvelinalustat ovat hyvin tuettuina hieman eksoottisempienkin käyttöjärjestelmien osalta. Myös sovellusten valvontaan löytyy hyvin tukea. Valvottavien laitteiden ja palveluiden listaus ei tuotakaan merkittäviä eroja järjestelmien välille. Ainoastaan EM7:n osalta ominaisuuslistaus on hieman muita lyhempi, mutta tarjolla olevat laajennukset näyttävät kurovan tätäkin eroa umpeen. Toki kaikki valvottavat järjestelmät eivät edes vaadi suoraa tukea vaan niitä voidaan monitoroida geneeristen valvontamenetelmien, kuten HTTP-kyselyiden avulla.

Toinen merkittävä tekninen tekijä on valvontajärjestelmien arkkitehtuuri. Arkkitehtuurin olennaisimpia piirteitä on hajautettu ja skaalautuva rakenne, jonka osat kykenevät keskenään salattuun viestintään. Arkkitehtuurin osalta Nimsoft, Hyperic ja Pandora tarjoavat hajautetumpaa rakennetta, ja EM7 pyrkii tarjoamaan monoliittisempaa ratkaisua. Suorituskyvyn ja skaalautuvuuden osalta kaikkien järjestelmien pitäisi venyä helposti tuhansien kohteiden valvontaan. Nimsoft ja Hyperic ovat vertailluista tuotteista ne, jotka panostavat agenttien käyttöön valvonnassa. Pandora ja EM7 ovat pääasiallisesti agentittomia, mutta tukevat tarvittaessa myös agentteja.

Tuotteiden eroja voidaan hakea myös käyttömallien mukaan. Kaikki valmistajat mainostavat toki koko it-infrastruktuurin valvontaa, mutta painopisteissä on hieman eroja. Nimsoftin fokus on palvelinten ja palveluiden valvonnassa. Hyperic on erikoistunut sovellusten, sovelluspalvelinten ja VMWaren valvontaan. Pandoran ja EM7:n painopiste on puolestaan verkon ja verkkolaitteiden valvonnassa. Kohderyhmiä tarkastellessa Hyperic ja Pandora ovat ainakin dokumentaationsa mukaan enemmän enterprise- kuin multi-tenant-tyyppisiä, vaikka tukevatkin datan ja näkymien eriyttämistä eri käyttäjäryhmille. Nimsoft ja EM7 puolestaan ovat enemmän palvelutuotannon näkökulmasta mietittyjä tuotteita.

Käyttöliittymän ominaisuuksien osalta tutkimuksen vertailu on haasteellista. Yleensä käyttöliittymän osalta esitellään erilaisia dashboard-näkymiä, joissa näkyy varsin korkean tason näkymiä valvottavan infrastruktuurin tilasta. Ylläpidon kontakti järjestelmään on kuitenkin pääasiassa hälytyskonsolin valvontaa ja valvontaparametrien konfigurointia. Joillakin järjestelmätoimittajilla on verkkosivuillaan tarjolla demoversio käyttöliittymästä, joilla voi kokeilla esimerkiksi hälytysnäkymän toimivuutta. Pandoran tarjoama käyttöliittymädemo oli erittäin hyödyllinen ja valaiseva verrattuna Hypericin ja ScienceLogicin tarjoamiin videoihin ja kuviin. Käyttäjäkohtaisen näkymän hallinta ja portaalin julkaisu asiakkaalle onnistuu kaikilla tuotteilla. Datan esityksen osalta ScienceLogicin käyttöliittymä vaikutti monipuolisimmalta, erityisesti hälytysdatan osalta.

Hälytysparametrien asetusta ja muita konfigurointitehtäviä ei markkinointimateriaaleissa juuri esitellä. Hypericin ja Pandoran osalta konfigurointi on käsitelty dokumentaatiossa ja vaikuttaa tapahtuvan yksinkertaisemmin kuin Nimsoftissa. ScienceLogicin konfigurointia sivutaan valmistajan esittelyvideolla ja sekin vaikuttaa toimivan hieman Nimsfotia helpommin. Toisaalta Nimsoftin probet tarjoavat palvelin ja sovellusvalvontaan enemmän parametrejä ja säätömahdollisuuksia kuin kilpailijansa.

Eräs huomionarvoinen seikka vertailluissa tuotteissa oli käyttäjäyhteisöjen olemassaolo ja aktiivisuus. Vaikka valvontajärjestelmälle ostetaankin tukipalvelua, käyttäjäyhteisöstä voi monissa tilanteissa löytyä arvokasta lisätietoa. Esimerkiksi jotkin tärkeät toiminnot ovat itsekehitettävien integraatioiden varassa ja muilta käyttäjiltä voi löytyä toteutukseen arvokasta tietoa. Myös ongelmatilanteissa ratkaisu saattaa löytyä suoraan tukifoorumeilta. Nimsoftin, Hypericin ja Pandoran tukifoorumit ovat ainakin viestimääriensä ja viestien tuoreuden perusteella kohtalaisen aktiivisia. EM7:n osalta forumeista ei löytynyt mainintaa.

Edellä mainittujen kriteerien perusteella on vaikea suositella valvontajärjestelmän toimittajan vaihtoa teknisillä syillä. Vertailun mukaan Nimsoft tarjoaa varsin hyvät ominaisuudet Appelsiinin tarpeisiin nähden, eikä mikään tutkituista vaihtoehtoisista tuotteista tuo merkittävää teknistä lisäarvoa. Ehkä ainoa parannus saataisiin aikaan käyttöliittymän ominaisuuksissa, kuten hälytysten hallinnassa ja raportointiominaisuuksissa. Hinnoittelu saattaa toki muuttaa asetelmaa merkittävästikin, mutta hintoja tarkemmin tuntematta on mahdotonta arvioida, millä aikavälillä säästöjä alkaisi syntyä huomioiden järjestelmän vaihtamisesta väistämättä syntyvät kulut.

Tämän tutkimuksen jatkoksi olisi luontevaa valita nyt vertailluista järjestelmistä yksi tai kaksi, jotka asennettaisiin testiympäristöön koekäyttöön. Koekäyttöjakson aikana järjestelmistä saataisiin tarkempaa tietoa oikeaa käyttöä simuloivilla testeillä niin varsinaisen valvontatoiminnallisuuden kuin käyttöliittymänkin osalta. Ainakin Hypericistä ja Pandorasta on saatavilla ilmaiset, täyden toiminnallisuuden versiot.

Lähteet

1 ITIL Service Design (v3). 2007. London: TSO.

2 Josephsen, David. 2007. Building a monitoring infrastructure with Nagios. Boston: Pearson Education, Inc.

3 CA Nimsoft Monitor Getting Started Guide 7.00. 2013. Verkkodokumentti. CA Technologies. <http://docs.nimsoft.com/prodhelp/en_US/Monitor/7.0/NimsoftMonitorGetting StartedGuide/NimsoftMonitorGetting StartedGuide7.00.pdf >. Luettu 20.11.2013.

4 CA Nimsoft Monitor Server Installation Guide. 2013. Verkkodokumentti. CA Technologies. <http://docs.nimsoft.com/prodhelp/en_US/Monitor/7.1/NimsoftMonitorServerInstallationGuide/NimsoftServerInstallationGuide-7.1.pdf >. Luettu 1.12.2013.

5 Leading Analyst Firm Ranks NetScout as the Top Vendor in the Worldwide Network Management Software and Appliance Market. Verkkodokumentti. Netscout. <http://www.netscout.com/company/news/press_releases_2013/pages/0711.aspx>. Luettu 1.12.2013.

6 CA Technologies Named the Worldwide Network Management Software and Appliance Market Share Leader by Market Research Firm. Verkkodokumentti. CA Technologies. < http://www.ca.com/us/news/press-releases/na/2012/ca-technologies-named-the-worldwide-network-management-software.aspx >. Luettu 1.12.2013.

7 Comparison of network monitoring systems. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems>. Luettu 1.12.2013.

8 VMware to Acquire SpringSource. 2009. Verkkodokumentti. VMWare. < http://www.vmware.com/company/news/releases/springsource.html >. Luettu 24.12.2013.

9 SpringSource. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/SpringSource>. Luettu 24.12.2013.

10 Hyperic acquisition binds Spring Framework to cloud. 2009. Verkkodokumentti. The Register. <http://www.theregister.co.uk/2009/05/04/springsource_hyperic_acquisition/>. Luettu 24.12.2013.

11 vCenter Hyperic Overview. 2013. Verkkodokumentti. VMWare. <http://pubs.vmware.com/hyperic-58/topic/com.vmware.ICbase/PDF/vcenter-hyperic-58-overview.pdf>. Luettu 7.1.2014.

12 Hyperic HQ Screenshots. 2012. Verkkodokumentti. VMWare. <http://www.hyperic.com/demo/monitoring-screenshots>. Luettu 26.12.2013.

13 Hyperic HQ 4.0 Product Tour. 2009. Verkkodokumentti. VMWare. <http://support.hyperic.com/download/attachments/59375779/HypericHQTour.pdf?version=1>. Luettu 3.12.2013.

14 Ártica. 2012. Verkkodokumentti. Ártica. <http://www.artica.es>. Luettu 16.12.2013.

15 Pandora FMS Architecture Overview. 2012. Verkkodokumentti. Ártica. <http://pandorafms.com/Pandora/architecture/downloads/PandoraFMS_Architecture_Overview.pdf >. Luettu 16.12.2013.

16 Pandora FMS 5.0 usage and management manual. 2013. Verkkodokumentti. Ártica. <http://sourceforge.net/projects/pandora/files/Pandora%20FMS%205.0/Final/Documentation/PandoraFMS_5.0_Manual_EN.pdf/download >. Luettu 17.12.2013.

17 Pandora FMS Features. 2013. Verkkodokumentti. Ártica. <http://pandorafms.com/Producto/Features/en>. Luettu 6.1.2014.

18 Online demo. 2013. Verkkodokumentti. Ártica. <http://pandorafms.com/Producto/demo/en>. Luettu 1.1.2014.

19 Review: ScienceLogic – One Network Management Tool to Rule Them All?. 2013. Verkkodokumentti. Packet Pushers. <http://packetpushers.net/review-sciencelogic-one-network-management-tool-to-rule-them-all/>. Luettu 27.12.2013.

20 Review: The best network monitoring system on earth. 2013. Verkkodokumentti. Infoworld. <http://www.infoworld.com/d/data-center/review-the-best-network-monitoring-system-earth-212335?page=0,0>. Luettu 27.12.2013.

21 ScienceLogic Server Monitoring. 2013. Verkkodokumentti. ScienceLogic. <http://www.sciencelogic.com/product/server-monitoring>. Luettu 27.12.2013.

22 After 10 years, MySQL still best for ScienceLogic's growing data demands. 2013. Verkkodokumentti. MySQL. <http://www.mysql.com/why-mysql/case-studies/mysql-best-for-sciencelogic.html>. Luettu 27.12.2013.

23 ScienceLogic System Management. 2013. Verkkodokumentti. ScienceLogic. <http://www.sciencelogic.com/sites/default/files/content-documents/sciencelogic-data-sheet-it-operations-cloud-management.pdf>. Luettu 30.12.2013.

24 ScienceLogic Next Generation IT Monitoring. 2013. Verkkodokumentti. ScienceLogic. <http://www.sciencelogic.com/sites/default/files/content-documents/sciencelogic-brochure.pdf>. Luettu 30.12.2013.

25 ScienceLogic for Service Providers. 2013. Verkkodokumentti. ScienceLogic. <http://www.sciencelogic.com/sites/default/files/content-documents/sciencelogic-brochure-service-providers.pdf>. Luettu 30.12.2013.